УДК 519.714

НИЖНИЕ ОЦЕНКИ ФОРМУЛЬНОЙ СЛОЖНОСТИ СИММЕТРИЧЕСКИХ БУЛЕВЫХ ФУНКЦИЙ

Д. Ю. Черухин

Аннотация. Для почти всех симметрических булевых функций, в частности, для функции голосования, получены нижние оценки сложности вида $\Omega(n \log n)$ при реализации их формулами в произвольном конечном базисе.

Работа посвящена получению нижних эффективных оценок сложности булевых функций [1]. В качестве средств реализации функций рассматриваются формулы (суперпозиции) в произвольном конечном базисе. В качестве реализуемых функций берутся симметрические булевы функции.

Функция называется *симметрической*, если при любых взаимно-однозначных перестановках ее аргументов значение функции сохраняется. Каждой симметрической булевой функции f от n аргументов взаимно-однозначно соответствует *характеристический набор* $(f_0, \ldots, f_n)$, в котором f_i, $0 \leqslant i \leqslant n$, является значением функции f на любом наборе, содержащем ровно i единиц. Функция голосования — это симметрическая функция от нечетного числа аргументов, характеристический набор которой имеет вид $(0, \ldots, 0, 1, \ldots, 1)$, причем число нулей в нем равно числу единиц.

Нижние оценки сложности симметрических функций в базисе $\{\&, \vee, \neg\}$ можно получать в помощью методов Б. А. Субботовской [2] и В. М. Храпченко [3]. Для базиса, состоящего из всех двуместных функций, нижние оценки вида $\Omega(n \log n)$ для почти всех симметрических функций (в частности, для функции голосования) были получены М. Дж. Фишером, А. Р. Мейером и М. С. Патерсоном [5]. П. Пудлак [7], усовершенствовав метод Л. Ходеса и Е. Шпекера [6], получил для всех симметрических функций, за исключением 16-ти, нижние оценки вида $\Omega(n \log \log n)$ в произвольном конечном базисе (16 исключительных функций имеют линейную сложность). В данной работе мы получим нижние оценки вида $\Omega(n \log n)$ для почти всех симметрических функций в произвольном конечном базисе. Верхние оценки сложности вида $n^{O(1)}$ для всех симметрических функций в произвольном конечном базисе были впервые получены В. М. Храпченко [4].

Булевой функцией n аргументов называется произвольная функция $f : \{0,1\}^n \to \{0,1\}$ при $n \in \mathbb{N}$, или константа (0 или 1) при $n = 0$. Множество всех булевых функций n аргументов обозначим через $P_2(n)$, множество всех функций от не более чем n аргументов — через $P_2^*(n)$. Зафиксируем счетное множество символов $\mathbb{X} = \{x_1, x_2, \ldots\}$, которые будем называть *переменными*. Каждому аргументу функции f поставим в соответствие переменную, а именно, для каждого i, $1 \leqslant i \leqslant n$, i-му аргументу сопоставим переменную x_i. Переменные, сопоставленные аргументам функции f, будем называть переменными функции f, их множество обозначим через $V(f)$, их число — через $n(f)$.

Пусть $Б$ — конечное функционально полное множество булевых функций. Такое множество назовем *базисом*. *Формулами* в базисе $Б$ называются следующие выражения и только они:

1) c, где c — символ константы и $c \in Б$;

2) $f(F_1, \ldots, F_n)$, где f — символ функции n аргументов, $n \geqslant 1$, $f \in Б$, каждое из выражений $F_1, \ldots, F_n$ является либо ранее построенной формулой в базисе $Б$, либо переменной.

Если формула не содержит переменных, то естественным образом определено ее *значение* — константа из множества $\{0, 1\}$. Две формулы называются *тождественно равными*, если при любом замещении в них всех переменных константами (при этом одинаковые переменные замещаются одинаковыми константами) значения полученных формул совпадают. Скажем, что формула F *реализует* функцию f от n аргументов, если формулы F и $f(x_1, \ldots, x_n)$ тождественно равны.

Пусть F — формула в базисе $Б$. Для произвольной переменной y обозначим через $L_y(F)$ количество вхождений переменной y в формулу F. Обозначим через $V(F)$ множество всех переменных, входящих в F хотя бы один раз, положим $n(F) = |V(F)|$. Пусть p — натуральное число, Y — конечное множество переменных. Введем две числовые характеристики формулы F — ее *сложность* $L(F)$ и *меру избыточности* с параметрами p и Y — $M_{p,Y}(F)$ следующим образом:

$$L(F) = \sum_{y \in V(F)} L_y(F), \qquad M_{p,Y}(F) = \sum_{y \in Y} \left(\frac{1}{p}\right)^{L_y(F)}.$$

Лемма 1. Пусть F — формула, $p \geqslant 2$, Y — конечное непустое множество переменных мощности n, и $V(F) \subseteq Y$. Тогда

$$L(F) \geqslant n \log_p \left(\frac{n}{M_{p,Y}(F)}\right). \tag{1}$$

Доказательство. Функция действительного аргумента $\chi(x) = \left(\frac{1}{p}\right)^x$ выпукла, поэтому в силу неравенства Иенсена имеем

$$\left(\frac{1}{p}\right)^{\frac{1}{n}L(F)} = \left(\frac{1}{p}\right)^{\frac{1}{n}\sum\limits_{y \in Y} L_y(F)} \leqslant \frac{1}{n}\sum_{y \in Y}\left(\frac{1}{p}\right)^{L_y(F)} = \frac{1}{n} M_{p,Y}(F).$$

Прологарифмировав по основанию p, получим

$$-\frac{L(F)}{n} \leqslant \log_p \left(\frac{M_{p,Y}(F)}{n}\right).$$

Отсюда следует (1). Лемма 1 доказана.

Сложностью функции f в базисе $Б$ (обозначение: $L_Б(f)$) называется минимальная из сложностей формул в базисе $Б$, реализующих функцию f. *Мерой избыточности функции* f в базисе $Б$ с параметром p (обозначение: $M_{Б,p}(f)$) называется число $\max M_{p,V(f)}(F)$, где максимум берется по всем тем формулам F в базисе $Б$, которые реализуют функцию f и содержат только переменные функции f (т. е. $V(F) \subseteq V(f)$).

Пусть k — наибольшее из чисел $n(f)$, $f \in Б$. Тогда $Б \subseteq P_2^*(k)$. Если мы получим нижнюю оценку сложности для формул в базисе $P_2^*(k)$, то не меньшая оценка будет справедлива для формул в базисе $Б$. Поэтому ограничимся случаем, когда $Б = P_2^*(k)$ (в силу функциональной полноты имеем $k \geqslant 2$).

Следствие из леммы 1. Пусть $Б = P_2^*(k)$, $p \geqslant 2$, f — функция n аргументов, $n \geqslant 1$. Тогда

$$L_Б(f) \geqslant n \log_p \left(\frac{n}{M_{Б,p}(f)} \right).$$

Доказательство. Пусть F — формула в базисе $Б$, реализующая функцию f и имеющая сложность $L(F) = L_Б(f)$. Тогда F не содержит переменных, несущественных для функции f. В противном случае, заменив несущественные переменные одинаковыми константами (базис $P_2^*(k)$ содержит константы), мы бы получили формулу меньшей сложности, реализующую функцию f в базисе $Б$. Таким образом, $V(F) \subseteq V(f)$. В силу (1) и неравенства $M_{p,V(f)}(F) \leqslant M_{Б,p}(f)$ имеем

$$L_Б(f) = L(F) \geqslant n \log_p \left(\frac{n}{M_{p,V(f)}(F)} \right) \geqslant n \log_p \left(\frac{n}{M_{Б,p}(f)} \right).$$

Следствие доказано.

Пусть $A = \{(y_1, c_1), \ldots, (y_m, c_m)\}$, где $y_1, \ldots, y_m$ — попарно различные переменные, $c_1, \ldots, c_m$ — константы из множества $\{0, 1\}$. Множество A назовем *подстановкой констант*. Количество нулей среди $c_1, \ldots, c_m$ обозначим через $N_0(A)$, количество единиц — через $N_1(A)$. Положим $\delta(A) = |N_0(A) - N_1(A)|$, $V(A) = \{y_1, \ldots, y_m\}$. Число $\delta(A)$ назовем *дефектом* подстановки констант A.

Сопоставим подстановке констант A взаимно-однозначное отображение $\Theta_A : \mathbb{X} \backslash V(A) \to \mathbb{X}$ следующим образом. Для произвольных i и j соотношение $\Theta_A(x_i) = x_j$ выполнено тогда и только тогда, когда $x_i \notin V(A)$ и $|\{x_1, \ldots, x_i\} \backslash V(A)| = j$ (другими словами, Θ_A осуществляет преобразование последовательности $x_1, x_2, \ldots$, при котором те переменные, которые входят в множество $V(A)$, удаляются из нее, а их места занимают оставшиеся переменные, не изменяя порядка своего следования).

Обозначим через $F|_A$ формулу, полученную из F заменой всех вхождений переменных $y_1, \ldots, y_m$ на константы $c_1, \ldots, c_m$ соответственно. Посредством $F|_A^*$ обозначим формулу, полученную из $F|_A$ переименованием переменных, при котором каждая переменная $x_i, x_i \notin V(A)$, заменяется на переменную $\Theta_A(x_i)$. Пусть f — функция n аргументов и $V(A) \subseteq V(f)$. Тогда через $f|_A$ обозначим функцию от n аргументов, реализуемую формулой $f(x_1, \ldots, x_n)|_A$. Посредством $f|_A^*$ обозначим функцию от $n - |A|$ аргументов, реализуемую формулой $f(x_1, \ldots, x_n)|_A^*$.

На множестве подстановок констант определим операцию $\circ$. Пусть A и B — произвольные подстановки констант. Положим

$$A \circ B = A \cup \{(y, c) \mid \exists x_i \ (x_i, c) \in B \ \& \ x_i = \Theta_A(y)\}.$$

Тогда для любой формулы F и любой функции f выполнено $(F|_A^*)|_B^* = F|_{A \circ B}^*$, $(f|_A^*)|_B^* = f|_{A \circ B}^*$.

Скажем, что функция f *линейно зависит* от переменной y, если f представима в виде $y \oplus g(\tilde{z})$, причем y не входит в набор переменных $\tilde{z}$. Функция, линейно зависящая от всех своих существенных переменных, называется *линейной*. Скажем, что функция f *сильно зависит* от переменной y, если для любой подстановки констант A, $V(A) = V(f) \backslash \{y\}$, функция $f|_A$ существенно зависит от y. Заметим, что f сильно зависит от y тогда и только тогда, когда f линейно зависит от y.

Лемма 2. Пусть $Б = P_2^*(k)$, $p = 2^k - 1$, f — нелинейная функция. Тогда существует подстановка констант A, обладающая следующими свойствами:

$$0 < |A| < n(f), \qquad \delta(A) \leqslant k + 1, \tag{2}$$

$$M_{Б,p}(f) \leqslant M_{Б,p}(f|_A^*). \tag{3}$$

Доказательство. Рассмотрим произвольную формулу F в базисе $Б$, которая реализует функцию f, содержит только переменные функции f и имеет меру избыточности $M_{p,V(f)}(F) = M_{Б,p}(f)$. Пусть P — множество подформул формулы F, которые реализуют нелинейные функции (подформула — это часть формулы, состоящая из подряд идущих символов и являющаяся формулой). Тогда $F \in P$, поэтому P непусто. Рассмотрим минимальный (по включению подформул) элемент множества P и обозначим его через G.

Пусть $v_1, \ldots, v_a$ — все переменные, от которых функция, реализуемая формулой G, зависит линейно. Обозначим

$$H = G|_{\{(v_1,0),\ldots,(v_a,0)\}}, \qquad G_1 = \oplus(v_1, \ldots, \oplus(v_a, H)\ldots).$$

Тогда формулы G и G_1 тождественно равны, и при этом функция, реализуемая формулой H, нелинейна и линейно не зависит ни от одной своей переменной. Заменим в формуле F подформулу G на подформулу G_1 и полученную формулу обозначим через F_1. Очевидно, что

$$M_{p,V(f)}(F_1) \geqslant M_{p,V(f)}(F) = M_{Б,p}(f). \tag{4}$$

Формулу H представим в виде $H = g(H_1, \ldots, H_l)$, где g — функция l аргументов, $l \leqslant k$, $H_1, \ldots, H_l$ — формулы или переменные. Функции, реализуемые формулами $H, H_1, \ldots, H_l$ (или тождественно равные этим переменным), обозначим соответственно через $h, h_1, \ldots, h_l$.

Пусть T — произвольное подмножество множества $\{1, \ldots, l\}$. Обозначим через $W(T)$ множество всех переменных из $V(f)$, которые для любого t, $t \in T$, входят в формулу H_t, а для любого t', $t' \notin T$, не входят в формулу $H_{t'}$. Множества $W(T)$ при разных $T \subseteq \{1, \ldots, l\}$ попарно не пересекаются и в объединении дают все множество $V(f)$, поэтому

$$M_{p,V(f)}(F_1) = \sum_{T \subseteq \{1,\ldots,l\}} M_{p,W(T)}(F_1). \tag{5}$$

Выберем множество T_0 так, чтобы число $M_{p,W(T_0)}(F_1)$ было наибольшим среди чисел $M_{p,W(T)}(F_1)$, где $T \subseteq \{1, \ldots, l\}$, $T \neq \varnothing$. Тогда

$$M_{p,W(T_0)}(F_1) \geqslant \frac{1}{2^k - 1} \sum_{T \neq \varnothing} M_{p,W(T)}(F_1) = \frac{1}{p} \sum_{T \neq \varnothing} M_{p,W(T)}(F_1). \tag{6}$$

Пусть $W(T_0) = \{y_1, \ldots, y_r\}$, $V(H) \backslash W(T_0) = \{z_1, \ldots, z_q\}$, причем переменные $y_1, \ldots, y_r, z_1, \ldots, z_q$ попарно различны. Обозначим $\Lambda = y_1 \oplus \ldots \oplus y_r$. Каждая из функций h_i, $i = 1, \ldots, l$, представима в виде

$$h_i = \varphi_i(\Lambda) \oplus \Lambda_i(z_1, \ldots, z_q),$$

где $\varphi_i \in P_2(1)$, Λ_i — линейная функция. Функция h нелинейна, поэтому $n(H) \geqslant 1$, следовательно, $r \geqslant 1$. Если при этом $q = 0$, то функция h представима в виде $\varphi(\Lambda)$, $\varphi \in P_2(1)$, т. е. h линейна. В то же время h нелинейна, следовательно, $q \geqslant 1$.

Функция h линейно не зависит от переменной y_1, поэтому h сильно не зависит от y_1, а значит, существует такая подстановка констант B, $V(B) = V(H) \backslash \{y_1\}$, что функция $h|_B$ существенно не зависит от переменной y_1. В качестве E возьмем подмножество подстановки констант B, для которого $V(E) = V(H) \backslash W(T_0)$. Функция $h|_E$ представима в виде $\varphi'(\Lambda)$, $\varphi' \in P_2(1)$, поэтому, если $h|_E$ существенно зависит от переменной y_1, то и функция $h|_B$

существенно зависит от y_1, что не верно. Следовательно, функция $h|_E$ существенно не зависит от переменной y_1, а значит, она тождественно равна константе.

Пусть $E = \{(z_1, c_1), \dots, (z_q, c_q)\}$. Рассмотрим систему линейных уравнений

$$\Lambda_i(z_1, \dots, z_q) = \Lambda_i(c_1, \dots, c_q), \qquad i = 1, \dots, l. \tag{7}$$

Эта система совместна и ранг ее матрицы не больше числа уравнений, равного l. Поэтому среди переменных $z_1, \dots, z_q$ можно выделить такие u переменных, $u \geqslant q - l$, что произвольный набор их значений можно дополнить до решения системы (7), взяв некоторым образом значения оставшихся $q - u$ переменных.

Зафиксируем значения этих u переменных так, чтобы число нулей среди них отличалось от числа единиц не более, чем на 1. Дополним образовавшийся набор до решения системы (7). Получим некоторое решение $z_1 = d_1, \dots, z_q = d_q$, причем количества нулей и единиц в наборе $(d_1, \dots, d_q)$ отличаются не более, чем на $l + 1$. Положим $A = \{(z_1, d_1), \dots, (z_q, d_q)\}$. Тогда $\delta(A) \leqslant l + 1 \leqslant k + 1$. В то же время, $|A| \leqslant |V(H)| - r < n(f)$ и $|A| \geqslant q > 0$. Условия (2) выполнены.

Докажем неравенство (3). Имеем

$$h|_A = g(\varphi_1(\Lambda) \oplus \Lambda_1|_A, \dots, \varphi_l(\Lambda) \oplus \Lambda_l|_A) = g(\varphi_1(\Lambda) \oplus \Lambda_1|_E, \dots, \varphi_l(\Lambda) \oplus \Lambda_l|_E) = h|_E.$$

Функция $h|_E$ тождественно равна константе, поэтому и функция $h|_A$ тождественно равна константе. Заменим в формуле $F_1|_A$ подформулу $H|_A$ на эту константу и полученную формулу обозначим через F_2.

Для каждой переменной y, $y \in W(T_0)$, выполнено

$$L_y(F_1) \geqslant L_y(F_2) + 1. \tag{8}$$

В то же время,

$$M_{p,W(\varnothing)}(F_1) = M_{p,W(\varnothing)}(F_2). \tag{9}$$

Формула F_2 реализует функцию $f|_A$. Обозначим через F_3 формулу, полученную из F_2 заменой каждой переменной x_i, $x_i \notin V(A)$, на переменную $\Theta_A(x_i)$. Тогда формула F_3 реализует функцию $f|_A^*$, причем $V(F_3) \subseteq V(f|_A^*)$. Отсюда следует

$$M_{p,V(f)\setminus V(A)}(F_2) = M_{p,V(f|_A^*)}(F_3) \leqslant M_{Б,p}(f|_A^*). \tag{10}$$

Из (4), (5), (6), (8), (9) и (10) окончательно получим

$$M_{Б,p}(f) \leqslant M_{p,V(f)}(F_1) = M_{p,W(\varnothing)}(F_1) + \sum_{T \neq \varnothing} M_{p,W(T)}(F_1) \leqslant$$

$$\leqslant M_{p,W(\varnothing)}(F_1) + pM_{p,W(T_0)}(F_1) = M_{p,W(\varnothing)}(F_1) + p \sum_{y \in W(T_0)} \left(\frac{1}{p}\right)^{L_y(F_1)} =$$

$$= M_{p,W(\varnothing)}(F_1) + \sum_{y \in W(T_0)} \left(\frac{1}{p}\right)^{L_y(F_1)-1} \leqslant M_{p,W(\varnothing)}(F_2) + \sum_{y \in W(T_0)} \left(\frac{1}{p}\right)^{L_y(F_2)} =$$

$$= M_{p,V(f)\setminus V(A)}(F_2) \leqslant M_{Б,p}(f|_A^*).$$

Неравенство (3), а вместе с ним и лемма 2, доказаны.

Лемма 3. Пусть $Б = P_2^*(n)$, $p \geqslant 2$, f — функция n аргументов, $n \geqslant 1$, и $c \in \{0,1\}$. Тогда существует такая переменная y, $y \in V(f)$, что

$$M_{Б,p}(f) \leqslant \frac{n}{n-1} M_{Б,p}(f|^*_{\{(y,c)\}}). \tag{11}$$

Доказательство. Пусть F — формула в базисе $Б$, которая реализует функцию f, содержит только переменные функции f и имеет меру избыточности $M_{p,V(f)}(F) = M_{Б,p}(f)$. В качестве y возьмем ту переменную из множества $V(f)$, которая входит в формулу F наибольшее число раз. Тогда

$$M_{p,\{y\}}(F) \leqslant \frac{1}{n} M_{p,V(f)}(F). \tag{12}$$

Формула $F|^*_{\{(y,c)\}}$ реализует функцию $f|^*_{\{(y,c)\}}$ и $V(F|^*_{\{(y,c)\}}) \subseteq V(f|^*_{\{(y,c)\}})$, поэтому

$$M_{Б,p}(f|^*_{\{(y,c)\}}) \geqslant M_{p,V(f|^*_{\{(y,c)\}})}(F|^*_{\{(y,c)\}}) = M_{p,V(f)\setminus\{y\}}(F|_{\{(y,c)\}}) = M_{p,V(f)\setminus\{y\}}(F). \tag{13}$$

Из (12), (13) и равенства $M_{p,V(f)}(F) = M_{Б,p}(f)$ получим

$$M_{Б,p}(f|^*_{\{(y,c)\}}) \geqslant M_{p,V(f)\setminus\{y\}}(F) = M_{p,V(f)}(F) - M_{p,\{y\}}(F) \geqslant$$

$$\geqslant M_{p,V(f)}(F) - \frac{1}{n} M_{p,V(f)}(F) = \frac{n-1}{n} M_{p,V(f)}(F) = \frac{n-1}{n} M_{Б,p}(f).$$

Отсюда следует (11). Лемма 3 доказана.

Линейным диаметром порядка s функции f назовем величину $D_s(f) = \max n(f|^*_A)$, где максимум берется по всем таким подстановкам констант A, $V(A) \subseteq V(f)$, что $\delta(A) \leqslant s$ и функция $f|_A$ линейна (определение линейного диаметра порядков 0 и 1 дано в [5]).

Лемма 4. Пусть $Б = P_2^*(k)$, $p = 2^k - 1$, $s = k+1$, $\gamma = \frac{\ln(s+1)}{\ln(2s+1)}$, f — функция и n аргументов и $n \geqslant 1$. Тогда

$$M_{Б,p}(f) \leqslant n^\gamma (D_s(f))^{1-\gamma}.$$

Доказательство. Проведем индукцию по числу n.

Базис индукции: функция f линейна (сюда входит случай $n = 1$). В этом случае $D_s(f) = n$. Кроме того, для любой функции f имеет место неравенство $M_{Б,p}(f) \leqslant n$. Отсюда следует

$$M_{Б,p}(f) \leqslant n = n^\gamma n^{1-\gamma} = n^\gamma (D_s(f))^{1-\gamma}.$$

Индуктивный переход: функция f нелинейна и для любой функции f', для которой $n(f') < n$, лемма доказана. По лемме 2, существует такая подстановка констант A, что $0 < |A| < n$, $\delta(A) \leqslant s$ и

$$M_{Б,p}(f) \leqslant M_{Б,p}(f|^*_A). \tag{14}$$

Построим по индукции число b и подстановки констант $A_0, \ldots, A_b$.

Положим $A_0 = A$. Пусть A_i уже построена. Если функция $f|^*_{A_i}$ линейна или $\delta(A_i) = 0$, то положим $b = i$ и завершим построение. Если же функция $f|^*_{A_i}$ нелинейна и $\delta(A_i) > 0$, то примем за c ту константу, для которой $N_c(A_i) < N_{\bar{c}}(A_i)$ и применим к ней и функции $f|^*_{A_i}$ лемму 3. По лемме 3 найдем переменную y_i, $y_i \in V(f|_{A_i})$, которая удовлетворяет условию

$$M_{Б,p}(f|^*_{A_i}) \leqslant \frac{n(f|^*_{A_i})}{n(f|^*_{A_i}) - 1} M_{Б,p}((f|^*_{A_i})|^*_{\{(y_i,c)\}}).$$

Положим $A_{i+1} = A_i \circ \{(y_i, c)\}$. Тогда

$$M_{Б,p}(f|^*_{A_i}) \leqslant \frac{n(f|^*_{A_i})}{n(f|^*_{A_i}) - 1} M_{Б,p}(f|^*_{A_{i+1}}) = \frac{n(f|^*_{A_i})}{n(f|^*_{A_{i+1}})} M_{Б,p}(f|^*_{A_{i+1}}). \tag{15}$$

Указанный процесс построения конечен, так как на каждом шаге дефект подстановки констант A_i уменьшается на единицу. Таким образом, $b \leqslant \delta(A)$. Обозначим $B = A_b$. Собрав вместе неравенства (15) для $i = 0, 1, \ldots, b-1$, получим

$$M_{Б,p}(f|^*_A) \leqslant \frac{n(f|^*_{A_0})}{n(f|^*_{A_1})} \cdot \ldots \cdot \frac{n(f|^*_{A_{b-1}})}{n(f|^*_{A_b})} M_{Б,p}(f|^*_{A_b}) = \frac{n(f|^*_A)}{n(f|^*_B)} M_{Б,p}(f|^*_B). \tag{16}$$

На каждом шаге число $n(f|^*_{A_i})$ не меньше единицы, поэтому $n(f|^*_B) \geqslant 1$. Применив к функции $f|^*_B$ предположение индукции, получим

$$M_{Б,p}(f|^*_B) \leqslant (n(f|^*_B))^\gamma (D_s(f|^*_B))^{1-\gamma}. \tag{17}$$

Докажем неравенство

$$D_s(f|^*_B) \leqslant D_s(f). \tag{18}$$

Если функция $f|^*_B$ линейна, то $D_s(f|^*_B) = n(f|^*_B)$. В свою очередь, $\delta(B) \leqslant \delta(A) \leqslant s$, т. е. B — пример подстановки констант, дефект которой не превосходит s, для которой функция $f|^*_B$ линейна и $V(B) \subseteq V(f)$. По определению линейного диаметра, $D_s(f) \geqslant n(f|^*_B) = D_s(f|^*_B)$. В этом случае (18) верно.

Пусть теперь $f|^*_B$ — нелинейная функция. Тогда $\delta(B) = 0$. Раскрыв определение числа $D_s(f|^*_B)$, рассмотрим такую подстановку констант E, $V(E) \subseteq V(f|^*_B)$, что $\delta(E) \leqslant s$, функция $(f|^*_B)|^*_E$ линейна и $D_s(f|^*_B) = n((f|^*_B)|^*_E)$. Тогда подстановка констант $B \circ E$ обладает свойствами: $V(B \circ E) \subseteq V(f)$, $\delta(B \circ E) \leqslant \delta(B) + \delta(E) \leqslant s$ и функция $f|^*_{B \circ E} = (f|^*_B)|^*_E$ линейна. Поэтому $D_s(f) \geqslant n(f|^*_{B \circ E}) = D_s(f|^*_B)$, т. е. в любом случае неравенство (18) верно.

Из (14), (16), (17) и (18) следует

$$M_{Б,p}(f) \leqslant M_{Б,p}(f|^*_A) \leqslant \frac{n(f|^*_A)}{n(f|^*_B)} M_{Б,p}(f|^*_B) \leqslant \frac{n(f|^*_A)}{n(f|^*_B)} (n(f|^*_B))^\gamma (D_s(f|^*_B))^{1-\gamma} \leqslant$$

$$\leqslant \frac{n(f|^*_A)}{n(f|^*_B)} (n(f|^*_B))^\gamma (D_s(f))^{1-\gamma} = n^\gamma (D_s(f))^{1-\gamma} \frac{n(f|^*_A)}{n^\gamma (n(f|^*_B))^{1-\gamma}}. \tag{19}$$

Оценим последнюю дробь в (19). Обозначим $a = |A|$, $m = n(f|^*_B)$. Тогда $m \geqslant 1$, $n = m + a + b$, $n(f|^*_A) = m + b$. Разделив числитель и знаменатель на m, получим

$$\frac{n(f|^*_A)}{n^\gamma (n(f|^*_B))^{1-\gamma}} = \frac{m+b}{(m+a+b)^\gamma m^{1-\gamma}} = \frac{1 + b/m}{(1 + (a+b)/m)^\gamma} \leqslant$$

(применим неравенство $b \leqslant \delta(A) \leqslant |A| = a$)

$$\leqslant \frac{1 + b/m}{(1 + 2b/m)^\gamma}. \tag{20}$$

Исследуем функцию действительного аргумента $\psi(x) = \frac{1+x}{(1+2x)^\gamma}$, $x > -\frac{1}{2}$. Имеем

$$\psi'(x) = \frac{(1+2x)^\gamma - (1+x)2\gamma(1+2x)^{\gamma-1}}{(1+2x)^{2\gamma}} = \frac{1+2x-2\gamma(1+x)}{(1+2x)^{1+\gamma}} = \frac{2(1-\gamma)x + (1-2\gamma)}{(1+2x)^{1+\gamma}}. \quad (21)$$

При $x > -1/2$ знаменатель в (21) положителен, поэтому производная функции $\psi(x)$ имеет не более одного нуля и этот нуль первой степени. В то же время

$$\psi(s) = \frac{(1+s)}{(1+2s)^{\log_{(1+2s)}(1+s)}} = \frac{(1+s)}{(1+s)} = 1 = \psi(0),$$

поэтому нуль функции $\psi'(x)$ существует и расположен на отрезке $[0, s]$.

Оценим $\psi'(0)$. Имеем

$$1 - 2\gamma = 1 - 2\frac{\ln(s+1)}{\ln(2s+1)} = \frac{\ln(2s+1) - 2\ln(s+1)}{\ln(2s+1)} = \frac{\ln\left(\frac{2s+1}{(s+1)^2}\right)}{\ln(2s+1)} < 0,$$

поэтому $\psi'(0) < 0$, т. е. в окрестности точки 0 функция $\psi(x)$ убывает. В силу единственности нуля производной, существует такая точка x_0, $0 < x_0 < s$, что на отрезке $[0, x_0]$ функция $\psi(x)$ убывает, а на отрезке $[x_0, s]$ — возрастает. Таким образом, для любого x, $0 \leqslant x \leqslant s$, справедливо неравенство $\psi(x) \leqslant 1$.

Заметим, что $b/m \geqslant 0$. Кроме того, $b \leqslant \delta(A) \leqslant s$ и $m \geqslant 1$, а значит, $b/m \leqslant s$. Таким образом, $0 \leqslant b/m \leqslant s$, следовательно, $\psi(b/m) \leqslant 1$. Объединив выкладки (19) и (20), получим

$$M_{Б,p}(f) \leqslant n^\gamma (D_s(f))^{1-\gamma} \cdot \psi(b/m) \leqslant n^\gamma (D_s(f))^{1-\gamma}.$$

Индуктивный переход завершен. Лемма 4 доказана.

Теорема 1. Пусть $Б = P_2^*(k)$, f — функция n аргументов, $n \geqslant 1$. Тогда

$$L_Б(f) \geqslant C_k n \log_2 \left(\frac{n}{D_{k+1}(f)}\right),$$

где $C_k = \frac{1}{k}\left(1 - \frac{\ln(k+2)}{\ln(2k+3)}\right)$.

Доказательство. Обозначим $p = 2^k - 1$, $s = k+1$, $\gamma = \frac{\ln(s+1)}{\ln(2s+1)}$. Применив следствие из леммы 1 и лемму 4, получим

$$L_Б(f) \geqslant n \log_p \left(\frac{n}{M_{Б,p}(f)}\right) \geqslant n \log_p \left(\frac{n}{n^\gamma (D_s(f))^{1-\gamma}}\right) = n \log_p \left(\left(\frac{n}{D_s(f)}\right)^{1-\gamma}\right) =$$

$$= \frac{1-\gamma}{\log_2 p} n \log_2 \left(\frac{n}{D_s(f)}\right) \geqslant \frac{1-\gamma}{k} n \log_2 \left(\frac{n}{D_s(f)}\right) = C_k n \log_2 \left(\frac{n}{D_{k+1}(f)}\right).$$

Теорема 1 доказана.

Заметим, что[1] $C_k \sim \frac{1}{k \log_2 k}$, $k \to \infty$.

[1] Символ $\sim$ означает ««асимптотически равно»», символ $\succcurlyeq$ — ««больше или равно по порядку»».

Теорема 2. Пусть $Б = P_2^*(k)$, f — симметрическая функция n аргументов, $(f_0, \ldots, f_n)$ — ее характеристический набор, d — натуральное число, причем $d \leqslant [n/2]$. Пусть также симметрическая функция, соответствующая характеристическому набору $(f_{[n/2]-d}, \ldots, f_{[n/2]+d})$, нелинейна. Тогда если $n/d \to \infty$, то

$$L_Б(f) \succcurlyeq n \log_2 \left(\frac{n}{d}\right). \tag{22}$$

Доказательство. Обозначим через A подстановку констант, для которой $V(A) \subseteq V(f)$, $\delta(A) \leqslant k+1$, функция $f|_A^*$ линейна, и $D_{k+1}(f) = n(f|_A^*)$. Заметим, что функция $f|_A^*$ является симметрической, и ее характеристический набор имеет вид $(f_{N_1(A)}, \ldots, f_{n-N_0(A)})$. Если $N_1(A) \leqslant [n/2]-d$ и $n - N_0(A) \geqslant [n/2]+d$, то функция $f|_A^*$ нелинейна, так как функция, задаваемая характеристическим набором $(f_{[n/2]-d}, \ldots, f_{[n/2]+d})$, является ее подфункцией (т. е. представима в виде $(f|_A^*)|_E^*$, где E — подстановка констант). В то же время, функция $f|_A^*$ линейна, поэтому либо $N_1(A) > [n/2]-d$, либо $n - N_0(A) < [n/2]+d$. Из последнего неравенства следует $N_0(A) > n - [n/2] - d \geqslant [n/2] - d$.

Итак, мы имеем $\max(N_0(A), N_1(A)) > [n/2] - d$. В качестве c возьмем такую константу, что $N_c(A) \geqslant N_{\bar{c}}(A)$. Получим $N_c(A) > [n/2] - d$. В то же время $N_c(A) - N_{\bar{c}}(A) = \delta(A) \leqslant k+1$, поэтому

$$|A| = N_c(A) + N_{\bar{c}}(A) = 2N_c(A) - (N_c(A) - N_{\bar{c}}(A)) > 2([n/2] - d) - (k+1),$$

а значит,

$$D_{k+1}(f) = n(f|_A^*) = n - |A| < n - 2[n/2] + 2d + (k+1) \leqslant 2d + (k+2) \leqslant (k+4)d.$$

Применив теорему 1, получим

$$L_Б(f) \succcurlyeq n \log_2 \left(\frac{n}{D_{k+1}(f)}\right) > n \log_2 \left(\frac{n}{d}\right) - n \log_2(k+4) \sim$$

(используем условие $n/d \to \infty$)

$$\sim n \log_2 \left(\frac{n}{d}\right).$$

Теорема 2 доказана.

Например, пусть Γ^n — функция голосования от n аргументов и $n \geqslant 3$. Положим $d = 1$. Тогда набор $(\Gamma^n_{[n/2]-d}, \ldots, \Gamma^n_{[n/2]+d})$ имеет вид $(0, 0, 1)$. Он является характеристическим набором нелинейной функции $x_1 \& x_2$. По теореме 2 имеем

$$L_Б(\Gamma^n) \succcurlyeq n \log_2 n.$$

Теорема 3. Для любого базиса $Б$ и почти всех симметрических функций f от n аргументов выполнено

$$L_Б(f) \succcurlyeq n \log_2 n. \tag{23}$$

Доказательство. Существует лишь четыре набора $(f_{[n/2]-d}, \ldots, f_{[n/2]+d})$, которые являются характеристическими наборами линейных функций (это два набора, состоящих из одинаковых значений, и два набора, в которых чередуются нули и единицы). Поэтому общее количество симметрических функций f, удовлетворяющих при данном d условию теоремы 2, равно

$$2^{n+1-(2d+1)}(2^{2d+1}-4) \sim 2^{n+1}, \qquad d \to \infty,$$

т. е. при ограничениях $d \to \infty$ и $n/d \to \infty$ для почти всех симметрических функций и любого базиса $Б$ справедлива оценка (22). Выбрав $d = [\sqrt{n}]$, мы получим, что для почти всех симметрических функций выполнено (23).

Теорема 3 доказана.

При $k = 2$ утверждения, аналогичные теоремам 1 и 3, были доказаны (другим методом) М. Дж. Фишером, А. Р. Мейером и М. С. Патерсоном [5].

Автор выражает благодарность чл.-корр. РАН О. Б. Лупанову за внимание к работе.

Работа выполнена при финансовой поддержке РФФИ (проект 99–01–01175), ФЦП ««Интеграция»» (проект АО-110), Программы ««Университеты России»» (проект 992206) и Программы поддержки ведущих научных школ РФФИ (проект 00–15–96103).

ЛИТЕРАТУРА

1. Нигматуллин Р. Г. Сложность булевых функций. — М.: Наука, 1991. — 240 с.

2. Субботовская Б. А. О реализации линейных функций формулами в базисе $\vee$, &, $^{-}$ // Докл. АН СССР. — 1961.— Т. 136, No 3. — С. 553–555.

3. Храпченко В. М. Об одном методе получения нижних оценок сложности П-схем // Матем. заметки. — 1971. — Т. 10, No 1. — С. 83–92.

4. Храпченко В. М. О сложности реализации симметрических функций формулами // Матем. заметки. — 1972. — Т. 11, No 1. — С. 109–120.

5. Fischer M. J., Meyer A. R., Paterson M. S. $\Omega(n \log n)$ lower bounds on length of Boolean formulas // SIAM J. Comput. — 1982. — V. 11, No 3. — P. 416–427.

6. Hodes L., Specker E. Lengths of formulas and elimination of quantifiers // Contributions to mathematical logic. — Amsterdam: North-Holland, 1968. — P. 175–188. [Рус. пер. в кн.: Кибернетический сборник. Новая серия. Вып. 10. — М.: Мир, 1973. — С. 99–113.]

7. Pudlák P. Bounds for Hodes-Specker theorem // Lecture Notes in Computer Science. V. 171. — Berlin: Springer, 1984. — P. 421–445.